ON SEPARATING TRANSCENDENCY BASES FOR DIFFERENTIAL FIELDS

A. SEIDENBERG

Let F be an arbitrary ordinary differential field[1] of characteristic $p \neq 0$, and let $F\langle u_1, \cdots, u_n \rangle$ be a differential extension field of F of degree of differential transcendency t. In [1, p. 189], we stated a theorem which, as far as wording is concerned, is analogous to a well-known theorem of S. MacLane in ordinary algebra. This theorem of ours states that if $F\langle u_1, \cdots, u_n \rangle / F$ is separable, then some t of the u_i form a separating transcendency basis, i.e., for an appropriate relettering of the u_i, $F\langle u_1, \cdots, u_n \rangle$ is separable over $F\langle u_1, \cdots, u_t \rangle$. The object of the present note is to establish the following stronger version of that theorem.[2]

THEOREM. *If $F\langle u_1, \cdots, u_n \rangle / F$ is separable, then any transcendency basis of $F\langle u_1, \cdots, u_n \rangle / F$ is also a separating transcendency basis.*

PROOF. We first prove that any t of the u_i which form a transcendency basis also form a separating transcendency basis. The theorem will then follow for any transcendency basis $v_1, \cdots, v_t$ since obviously we may include the v_j amongst the u_i.

For $t=0$, there is nothing to prove. Confining ourselves to transcendency bases selected from the u_i, the theorem is also immediate for $t=n$. Consider next the case $t=n-1$, and let $u_1, \cdots, u_{n-1}$ be algebraically independent over F. By [1, p. 188, Theorem 6, Corollary], the u_{ij}, $i=1, \cdots, n-1$; $j=0, 1, \cdots$, are algebraically independent over F. By the definition in [1, p. 183], $F\langle u_1, \cdots, u_n \rangle$ is finite over $F\langle u_1, \cdots, u_{n-1} \rangle$, so for some d, u_{nd} is algebraic over $F\langle u_1, \cdots, u_{n-1} \rangle (u_{n0}, \cdots, u_{n,d-1})$. Let d be minimal, i.e., u_{ij}, u_{nk}, $i=1, \cdots, n-1$; $j=0, 1, \cdots$; $k=0, \cdots, d-1$, are algebraically

Presented to the Society, December 29, 1954; received by the editors October 27, 1954.

[1] Definitions, notation, and terminology will be as in [1].

[2] The proof of the weaker theorem in [1; p. 189], though essentially correct, is too compressed; and we would like to add one remark to that proof. Let G, U_{nr} be as in the proof; replacing G by a derivative if necessary, we may suppose G involves no proper derivative of U_{nr}. As $G(u_1, \cdots, u_{n-1}; u_{n0}, \cdots, u_{n,r-1}, U_{nr})=0$ is not necessarily a defining equation for u_{nr}, the separability of u_{nr} over $F\langle u_1, \cdots, u_{n-1} \rangle (u_{n0}, \cdots, u_{n,r-1})$ does not yet follow from the form of G. That separability would follow, however, if we had that $\partial G / \partial U_{nr} \neq 0$ for $U=u$: this we have because of the minimal degree of G. With this additional point in mind, it is not difficult to fill the slight gaps which occur in the proof as it now stands in [1].

independent over F, but u_{nd} is algebraically dependent on this set over F. Let A be the set of polynomials $\{G\}$ in the polynomial ring $F\{U_1, \cdots, U_n\}$ such that $G\neq 0$, G is of degree 0 in U_{ni}, $i>d$, and $G(u_1, \cdots, u_n)=0$. Let B be the subset of A consisting of the polynomials of minimum total degree. Let $G\in B$. The separability of $F\langle u_1, \cdots, u_n\rangle/F$ implies that $G\notin F[\cdots, U_{ij}^p, \cdots]$. Not all the U_{ni}, $i\leqq d$, occurring in G occur with exponent divisible by p. In fact, assume otherwise. Since not all the exponents occurring in G are divisible by p, at least one of the U_{jk}, $j=1, \cdots, n-1$, say U_{1h}, occurs in G with exponent not divisible by p; we may suppose that derivatives of U_{1h}, if they occur in G, occur with exponents divisible by p. The derivative G' of G also is in A and in B; so replacing G by a derivative if necessary, we may suppose G involves no proper derivative of U_{1h}. With these assumptions on G, we have: (1) degree of G' in $U_{1,h+1}$ is 1, degree of G' in U_{1j}, $j>h+1$, is 0; (2) coefficient of $U_{1,h+1}$ in G' does not vanish at $U=u$, since it is of too small degree to be in A. Hence $u_{1j}\in F\langle u_2, \cdots, u_{n-1}\rangle(u_{n0}^p, \cdots, u_{nd}^p; u_{10}, \cdots, u_{1,h})$, $j\geqq 0$. Since $F\langle u_1, \cdots, u_n\rangle/F\langle u_1, \cdots, u_{n-1}\rangle$ is finite, for some r, $r\geqq d$, we have $u_{nj}\in F\langle u_1, \cdots, u_{n-1}\rangle(u_{n0}, \cdots, u_{nr})$, $j\geqq 0$. This last field may be written as $F\langle u_2, \cdots, u_{n-1}\rangle(u_{n0}, \cdots, u_{nr}; u_{10}, \cdots, u_{1h})$, whence $F\langle u_1, \cdots, u_n\rangle/F\langle u_2, \cdots, u_{n-1}\rangle$ is finite. This contradicts the assumption $t=n-1$. Hence for any given $G\in B$, at least one U_{nj}, $j\leqq d$, occurs with exponent not divisible by p. Differentiating G sufficiently often we may suppose that U_{nd} occurs in G with exponent not divisible by p. Since u_{ij}, u_{nk}, $i=1, \cdots, n-1$; $j=0, 1, \cdots$; $k=0, \cdots, d-1$, are algebraically independent over F, we have that $G(u_{ij}, u_{nk}, U_{nd})=0$ is an irreducible (separable) equation for u_{nd} over $F(u_{ij}, u_{nk})$. Hence $F\langle u_1, \cdots, u_n\rangle$ is separable over $F\langle u_1, \cdots, u_{n-1}\rangle$. This completes the proof for $t=n-1$.

For $0<t<n-1$, we apply the Theorem of the Primitive Element. In the application, no separability condition is required (as in ordinary algebra—see the remarks in [1, p. 183, bottom of page]), but we do need to know, or rather, it would be sufficient to know, that $F\langle u_1, \cdots, u_t\rangle$, where $u_1, \cdots, u_t$ is any given transcendency basis, has no finite linear basis over its field of constants. Even if $F\langle u_1, \cdots, u_t\rangle$ had a finite linear basis over its field of constants, we could overcome this difficulty by the well-known device of adjoining an appropriate nonconstant element to $F\langle u_1, \cdots, u_n\rangle$. Here we may as well determine the constants of $F\langle u_1, \cdots, u_t\rangle$. If F_0 is the constant-field of F, then we shall see that the constant field of $F\langle u_1, \cdots, u_t\rangle$ is $F_0(\cdots, u_{ij}^p, \cdots)$. Assuming this for a moment we see that $F\langle u_1, \cdots, u_t\rangle$ has no finite linear basis over its field of constants,

whence $F\langle u_1, \cdots, u_n\rangle = F\langle u_1, \cdots, u_t; w\rangle$. By the case $t=n-1$, then, the basis $u_1, \cdots, u_t$ is separating.

Since $F\langle u_1, \cdots, u_t\rangle/F$ is separable, the u_{ij} are, as previously mentioned, algebraically independent: the converse is immediate.

LEMMA. *Let F be a differential field of characteristic $p\neq 0$, F_0 its field of constants, and assume that $F\langle u_1, \cdots, u_t\rangle/F$ is separable and of degree of differential transcendency t. Then $F_0(\cdots, u_{ij}^p, \cdots)$, $i=1, \cdots, t; j=0, 1, \cdots$, is the field of constants of $F\langle u_1, \cdots, u_t\rangle$.*

PROOF. Let $P(u)/Q(u) \in F\langle u_1, \cdots, u_t\rangle$ be a constant $\neq 0$, where $P(u)$, $Q(u)$ are elements of the *polynomial ring* $F\{u_1, \cdots, u_t\}$, and P and Q have no common factor of positive degree. We first assert that $P, Q \in F[\cdots, u_{ij}^p, \cdots]$. For suppose this is not the case, and say $Q \notin F[\cdots, u_{ij}^p, \cdots]$. Then Q' is not zero, and $P/Q = P'/Q'$. Since degree of P = degree of P' and degree of Q = degree of Q', we get $P' = dP$, $Q' = dQ$ for some $d \in F$, $d \neq 0$. Repeating the argument, we get $P^{(i)} = d_iP$, $Q^{(i)} = d_iQ$, where $d_i \in F$ and the superscript indicates the ith derivative. Since $Q^{(i)}$ for sufficiently high i involves some u_{jk} not occurring in Q, we have a contradiction. Thus $Q \in F[\cdots, u_{ij}^p, \cdots]$, and similarly for P. Let $P = \sum a_i\pi_i^p$, $Q = \sum b_i\pi_i^p$, where a_i, $b_i \in F$, $a_ib_i \neq 0$, and the π_i are power products of the u_{jk} with $\pi_i \neq \pi_j$ for $i \neq j$. If $Q' = 0$, then each b_i is a constant, since $Q' = \sum b_i'\pi_i^p = 0$; and likewise the a_i are constant; so $P(u)/Q(u)$ has the required form if $Q' = 0$. Assume $Q' \neq 0$: then as above we have $P' = dP$, $Q' = dQ$, $d \in F$, $d \neq 0$. This yields $a_i' = da_i$, whence any two a_i have a constant ratio. Thus $P = e\sum a_i\pi_i^p$, $Q = f\sum b_i\pi_i^p$, where now the a_i, b_i are in F_0. Since P/Q and $\sum a_i\pi_i^p / \sum b_i\pi_i^p$ are constants, so is e/f. Thus P/Q has the desired form. This completes the proof.

REFERENCE

1. A. Seidenberg, *Some basic theorems in differential algebra (characteristic p, arbitrary)*, Trans. Amer. Math. Soc. vol. 73 (1952) pp. 174–190.

UNIVERSITY OF CALIFORNIA, BERKELEY